Commissaire à
l'information et à
protection de la
vie privée/Ontario

Directives concernant la sécurité des transmissions par télécopieur

Ann Cavoukian, Ph.D.
Commissaire
Modifié en février 1999

103-03514/

Documents connexes

- Les principes de la vie privée pour les systèmes de courrier électronique
- Les principes de protection de la vie privée et la messagerie vocale

Commissaire à l'information et à la protection de la vie privée/Ontario

80, rue Bloor ouest
Bureau 1700
Toronto (Ontario)
M5S 2V1

416-326-3333
1-800-387-0073
Télécopieur : 416-325-9195
ATS (Téléimprimeur) : 416-325-7539
Site Web : www.ipc.on.ca

Le Bureau du commissaire remercie Nick Magistrale de sa contribution au présent document.

Cette publication est disponible sur le site Web du Bureau du commissaire. This publication is also available in English.

Table des matières

Introduction 1

Objet 2

Directives 3

Diviser les renseignements en catégories 3

Incidence de la technologie 3

Sensibiliser le personnel en adoptant des politiques et des procédures 4

Garantir la sécurité des transmissions 5

Assurer la sécurité matérielle 8

S'assurer que les télécopies parviennent à leur destinataire 8

Conclusion 10

Annexe A — Code des pratiques équitables en matière de renseignements 11

Introduction

Le télécopieur (que l'on appelle parfois « fax ») est une méthode de transmission d'information par ligne téléphonique ordinaire. Normalement, l'utilisateur place le document à télécopier dans l'alimenteur de documents du télécopieur et compose le numéro de téléphone du télécopieur destinataire. Ce dernier reçoit rapidement une copie du document. Un autre type de transmission par télécopieur consiste à envoyer un document à partir d'un ordinateur.

Malheureusement, il arrive que des documents soient transmis par inadvertance à un mauvais destinataire. Cette situation peut se produire si l'envoyeur compose un faux numéro ou si le destinataire n'est pas sur place pour recevoir le document et qu'une autre personne le prenne à sa place. Lorsqu'un tiers qui attend un document au télécopieur prend connaissance d'un document déjà arrivé, il y a également violation de la confidentialité. La *Loi sur l'accès à l'information et la protection de la vie privée* et la *Loi sur l'accès à l'information municipale et la protection de la vie privée* (les « *Lois* ») peuvent régir les situations de ce genre.

En effet, l'un des objets des *Lois* consiste à protéger les renseignements personnels dont les organismes gouvernementaux ont la garde. Or, ces organismes envoient souvent des renseignements personnels par télécopieur. Conscient des risques qui en découlent, le Bureau du commissaire à l'information et à la protection de la vie privée (le « Bureau du commissaire ») a publié en juin 1989 le document *Directives concernant la sécurité des transmissions par télécopieur*. Les organismes gouvernementaux ont été invités à consulter ces directives aux fins de l'élaboration de systèmes et de procédés visant à protéger la confidentialité des renseignements transmis par télécopieur. Ces directives ont été très bien accueillies, et des centaines d'exemplaires ont été commandés.

En février 1990, le Secrétariat du Conseil de gestion du gouvernement de l'Ontario a publié une directive concernant la gestion des mesures de sécurité informatiques, qui avait notamment pour but de veiller à ce que les ministères protègent la confidentialité, l'intégrité et la disponibilité des données créées, stockées, traitées ou communiquées par voie informatique, y compris par télécopieur.

Parmi les principes énoncés dans ce document figurait la nécessité de faire conformer la sécurité informatique aux exigences de la *Loi sur l'accès à l'information et la protection de la vie privée* en matière de vie privée et de confidentialité. Cette mention révèle que les principes de la protection de la vie privée feront partie intégrante des mesures de sécurité informatique dans le secteur public, et qu'ils seront conformes aux directives du Bureau du commissaire concernant les transmissions par télécopieur.

La popularité des télécopieurs ne cesse de croître, de même que leur variété et leur complexité. Comme les autres technologies de communication, ils ont subi des changements rapides. En outre, la puissance des ordinateurs connaît une hausse fulgurante, de même que l'usage de réseaux, Internet et le nombre croissant de fournisseurs Internet offrant des services en ligne ont également une incidence considérable sur la sécurité des transmissions par télécopieur. Pour toutes ces raisons, le Bureau du commissaire a préparé cette nouvelle édition de ses directives. Le présent document est fondé sur un code de pratiques équitables en matière de renseignements qui représente la pierre angulaire de la protection de la vie privée. Ce code est fourni à l'annexe A.

Objet

Le présent document propose des directives à l'usage des organismes gouvernementaux aux fins de l'élaboration de systèmes et de procédures visant à protéger la confidentialité et l'intégrité des renseignements transmis par télécopieur. Les entreprises privées pourraient également les juger utiles.

Ces directives visent à assurer l'adoption de pratiques acceptables en matière de vie privée (en veillant à ce que les renseignements délicats et personnels ne soient accessibles qu'aux personnes autorisées) et à éviter le recours à des pratiques indésirables (p. ex., problèmes de protection de la vie privée, de sécurité ou de confidentialité).

Le présent document ne traite pas de la totalité des nouvelles technologies ou des nouveaux produits liés à la télécopie, et ne contient aucune recommandation quant aux produits, marques ou fournisseurs.

Directives

Diviser les renseignements en catégories

Tous les renseignements que détiennent les organismes gouvernementaux ne nécessitent pas le même degré de protection lors de leur communication. La première étape de l'élaboration de directives consiste donc à diviser en catégories ces divers types de renseignements.

Ces catégories peuvent être fondées sur les *Lois*. Ainsi, les documents dont un organisme gouvernemental a la garde ou le contrôle en Ontario peuvent représenter :

- des renseignements personnels (article 2 des *Lois*);
- des documents visés par des exceptions (prévues aux articles 12 à 22 de la *Loi* provinciale et aux articles 6 à 16 de la *Loi* municipale);
- des documents généraux (qui contiennent des renseignements qui ne sont pas personnels et qui ne sont pas visés par des exceptions).

La partie III de la *Loi* provinciale et la partie II de la *Loi* municipale portent sur la protection de la vie privée. Ces dispositions obligent les organismes gouvernementaux à empêcher l'utilisation non autorisée ou la divulgation des renseignements personnels qu'ils possèdent. Elles régissent également la collecte, l'utilisation, la divulgation et l'élimination des renseignements personnels.

Incidence de la technologie

L'évolution du télécopieur et l'usage croissant de l'ordinateur pour envoyer des télécopies procurent divers avantages aux utilisateurs :

- D'importantes bases de données contenant des listes de numéros de téléphone peuvent être constituées et utilisées pour envoyer des télécopies à des groupes de destinataires;
- La taille du document à envoyer ne représente plus un obstacle, et il n'est plus nécessaire qu'il soit imprimé;
- Presque tout renseignement stocké dans un ordinateur (p. ex., lettres, rapports, feuilles de calcul financières, photos) peut être télécopié;
- Le document à transmettre peut être composé de données provenant de diverses sources sauvegardées dans un ordinateur;
- Contrairement aux documents sur papier, les documents sauvegardés dans un ordinateur peuvent être modifiés très facilement avant la transmission ou après la réception;
- Il suffit d'avoir un ordinateur ainsi que le logiciel et le matériel nécessaire pour envoyer ou recevoir une télécopie.

Il est donc beaucoup plus facile qu'auparavant d'envoyer un document par télécopieur, mais ce mode d'envoi est maintenant plus difficile à surveiller. En effet, à cause des progrès technologiques, la télécopie présente de nouveaux risques. Par exemple, l'envoi de télécopies par ordinateur permet de supprimer les rapports d'activité, de sorte qu'il est essentiellement impossible de savoir ce qui a été télécopié et par qui.

Matériel et logiciels informatiques

De nos jours, les ordinateurs sont souvent équipés de modems télécopieurs. Les organismes qui achètent de tels appareils donnent à leurs employés la possibilité d'envoyer et de recevoir des télécopies à partir de leur poste de travail.

En outre, divers logiciels en vente sur le marché, notamment des logiciels de traitement de texte, sont dotés de fonctions de télécopie intégrées. Les versions récentes des systèmes d'exploitation tels OS/2 d'IBM et Microsoft Windows 95/98 comportent également pareilles fonctions.

Informatique mobile et communications sans fil

Les progrès dans l'informatique mobile et les communications sans fil suscitent de nouvelles inquiétudes concernant la transmission sûre de télécopies. Ainsi, un ordinateur portatif équipé du logiciel et du matériel nécessaire peut envoyer ou recevoir des télécopies au moyen d'un téléphone cellulaire. En outre, les télécopieurs portatifs et de poche peuvent être employés presque n'importe où.

Fournisseurs de services de télécopie

De nos jours, il n'est plus nécessaire d'avoir accès à un appareil pour télécopier un document. En effet, il est possible d'envoyer le document par courriel à un service de télécopie, qu'offrent la plupart des fournisseurs de services en ligne.

Sensibiliser le personnel en adoptant des politiques et des procédures

Des documents tels des curriculum vitae, des formulaires de demande et de commande, des propositions commerciales et des contrats contiennent des renseignements qui pourraient être utilisés à mauvais escient par des individus mal intentionnés. Il importe donc d'établir à l'intention du personnel des politiques et des procédures indiquant comment protéger la confidentialité des documents importants pendant leur transmission.

Les organismes doivent s'assurer que leurs politiques et procédures concernant les télécopies tiennent compte des considérations technologiques suivantes.

Utilisation de télécopieurs ordinaires

Dans les bureaux où l'on utilise des télécopieurs, une personne et un substitut devraient être chargés des télécopies. En cas de problème technique ou autre, le personnel pourra s'adresser à eux.

Le télécopieur devrait être placé à un endroit où :

- le public n'a pas accès;
- son utilisation peut être surveillée par la personne responsable;
- seul le personnel autorisé a accès aux documents transmis.

Il y a lieu d'élaborer des politiques et procédures claires concernant l'usage du télécopieur et d'en informer le personnel qui transmet ou reçoit des télécopies.

Envoi de télécopies par ordinateur

Dans nombre d'organismes, l'envoi et la réception de télécopies ne sont plus réservés aux personnes autorisées et se font souvent par ordinateur. Dans ce cas, le personnel devrait être informé des règles à suivre lorsqu'il transmet des renseignements personnels ou délicats.

Dans les organismes qui envoient ou reçoivent beaucoup de télécopies, il serait judicieux d'envisager l'installation d'un serveur de télécopies auquel ne pourront accéder que les personnes autorisées à envoyer et à recevoir des télécopies.

Encore une fois, il est souhaitable d'élaborer des politiques et procédures claires et de les communiquer à tout le personnel.

Garantir la sécurité des transmissions

Certains télécopieurs sont dotés de caractéristiques de sécurité qui permettent de mieux assurer la confidentialité des transmissions.

Rapports d'activité, dispositifs de verrouillage et boîtes de réception confidentielles

Presque tous les télécopieurs traditionnels impriment une confirmation de transmission après usage. Ce rapport confirme la transmission du document en indiquant le numéro de télécopieur du destinataire et le nombre de pages transmises. L'envoyeur devrait vérifier cette confirmation pour s'assurer que la transmission a été bel et bien effectuée.

Le destinataire, quant à lui, devrait vérifier s'il a bien reçu le nombre de pages indiqué sur le bordereau de transmission ou la confirmation (si aucun bordereau n'a été transmis). Si des pages sont manquantes, le destinataire devrait appeler l'envoyeur et lui demander de renvoyer ces pages.

La plupart des télécopieurs traditionnels peuvent également imprimer des rapports d'activité après une période donnée ou un certain nombre de transmissions ou de réceptions. Par exemple, le télécopieur peut être réglé pour imprimer un rapport toutes les 40 opérations. Ce rapport permet de contrôler l'utilisation du télécopieur. Cependant, la plupart des appareils ne permettent d'imprimer chaque rapport qu'une seule fois.

Il est donc possible pour un utilisateur non autorisé d'imprimer un rapport d'activité puis de le détruire, éliminant toute trace d'utilisations non permises. Par exemple, une personne pourrait prendre un document qui ne lui est pas destiné et supprimer toute mention de son arrivée en imprimant puis en détruisant le rapport d'activité.

Des caractéristiques telles que les dispositifs de verrouillage et les boîtes de réception confidentielles pourraient permettre de résoudre ce problème. Dans certains organismes, il est nécessaire de prévoir une protection supplémentaire pour les télécopies. Le télécopieur peut être équipé d'un dispositif de verrouillage qui, lorsqu'il est utilisé, empêche la transmission et la réception de télécopies. En installant un tel dispositif, l'organisme peut réserver l'usage du télécopieur à des personnes désignées.

Certains télécopieurs sont munis d'une boîte de réception confidentielle, c'est-à-dire d'une mémoire qui emmagasine les documents reçus. Pour imprimer ces documents, il faut entrer un mot de passe. Ainsi, seule une personne désignée peut recevoir la télécopie. En outre, l'appareil de l'envoyeur doit être en mesure de transmettre le document à un télécopieur muni d'une telle boîte de réception.

S'il faut envoyer des renseignements personnels par télécopieur en cas d'urgence, l'envoyeur devrait les transmettre uniquement dans une boîte de réception confidentielle et, si possible, utiliser une fonction de chiffrement. Les télécopies reçues par ordinateur devraient être automatiquement acheminées dans un répertoire auquel seules des personnes autorisées ont accès. Si l'on ne dispose pas de boîte de réception confidentielle ou de répertoire sécurisé, les renseignements personnels ou les documents faisant l'objet d'une exception ne devraient contenir aucun renseignement d'identification. Tous les télécopieurs dont les organismes gouvernementaux se servent pour transmettre des renseignements personnels ou délicats devraient être munis d'une boîte de réception confidentielle ou d'un dispositif de chiffrement.

Les différents services de l'organisme ne devraient pas utiliser le même télécopieur. Un tel usage partagé pourrait entraîner la divulgation de renseignements personnels ou délicats à des personnes non autorisées d'un autre service.

Certains télécopieurs sont équipés d'un dispositif de stockage permanent, comme un disque dur, pour protéger le contenu de la boîte de réception confidentielle en cas de panne de courant. Les données sauvegardées sur disque sont ainsi préservées.

Chiffrement

De nos jours, les télécopies sont transmises par ligne téléphonique ordinaire ou par l'entremise des réseaux cellulaires. Comme les conversations, les télécopies peuvent être interceptées en cours de transmission par des personnes non autorisées. En effet, il suffit pour ce faire d'obtenir du matériel facile d'accès et d'assemblage, au coût étonnamment bas.

Le meilleur moyen d'éviter ce problème consiste à chiffrer les données pour les rendre illisibles tant qu'elles n'ont pas été déchiffrées. Le Bureau du commissaire est d'avis que le chiffrement représente l'une des méthodes les plus efficaces pour empêcher que les données transmises ne soient interceptées et lues par des personnes non autorisées.

Actuellement, il est possible de chiffrer une télécopie en utilisant un chiffreur. Ce dispositif est en vente sous forme logicielle ou matérielle. Il génère et distribue automatiquement les clés de chiffrement nécessaires pour assurer une transmission sécurisée.

L'expéditeur et le destinataire doivent être munis du même chiffreur. Ce dispositif pourrait donc représenter une mesure de sécurité pratique pour un groupe « fermé » d'utilisateurs, notamment au sein d'un même service. Dans l'organisme, chaque groupe d'utilisateurs situé dans le même immeuble pourrait envisager de réserver un télécopieur aux transmissions chiffrées. Tous les organismes communiquant avec ce groupe pourraient alors utiliser le même type de chiffreur. De cette façon, si une télécopie était envoyée à un appareil dépourvu de chiffreur compatible, le destinataire ne pourrait lire le document. Des données chiffrées peuvent également être transmises d'un ordinateur à un autre, puis déchiffrées.

Il faut éviter de télécopier des renseignements personnels et des documents visés par une exception à moins d'utiliser un chiffreur au cas où les données seraient interceptées pendant la transmission. S'il est impossible de chiffrer le document, les renseignements personnels qu'il contient pourraient en être soustraits avant la télécopie.

Bien que cela ne soit pas recommandé, il pourrait être nécessaire de transmettre des renseignements personnels non chiffrés sans qu'il soit possible de supprimer les renseignements d'identification, et souvent, le télécopieur du destinataire n'est pas doté d'une boîte de réception confidentielle. Dans ce cas, l'expéditeur devrait donner un coup de fil au destinataire avant la transmission pour lui demander d'aller attendre l'arrivée du document et de confirmer sa réception par téléphone.

Cependant, la technologie du chiffrement a progressé, et il est désormais possible d'envoyer des renseignements personnels chiffrés grâce à des clés publiques.

Il existe maintenant sur le marché des produits qui permettent de s'assurer que les télécopies parviennent à leur destinataire sans être divulguées à des tiers ou à des personnes non autorisées. Certains appareils peuvent également vérifier l'identité de l'expéditeur et veiller à la confidentialité et à l'intégrité du message. Les organismes qui disposent d'appareils de ce genre peuvent déterminer les télécopies à envoyer ou à recevoir en mode sécurisé. Cette technologie authentifie l'expéditeur et le destinataire, puis chiffre les données pour une transmission sûre.

Photocopie des documents reçus par télécopieur

Certains anciens modèles de télécopieurs imprimaient les documents reçus sur du papier thermique. Comme les documents ainsi imprimés pâlissent progressivement, il est recommandé aux organismes qui se servent de ce papier de les photocopier afin de pouvoir les conserver pendant la période minimale prescrite. Les originaux sur papier thermique peuvent ensuite être détruits de façon sécuritaire. Les documents imprimés par des télécopieurs à jet d'encre ou au laser ne pâlissent pas.

Assurer la sécurité matérielle

L'environnement dans lequel est utilisé le télécopieur peut avoir une incidence considérable sur la sécurité des transmissions. Bien que les méthodes de travail s'améliorent progressivement, on place encore dans certains bureaux le télécopieur à un endroit relativement accessible au public, où presque tout le monde peut s'en servir. Les documents reçus peuvent alors être lus par des personnes non autorisées, et il est plus difficile de préserver la confidentialité des renseignements personnels ou de nature délicate.

En règle générale, l'expéditeur ignore dans quelles conditions ses documents seront reçus. Ainsi, il pourrait envoyer des renseignements confidentiels, croyant à tort que des mesures de sécurité sont en place au bureau du destinataire. C'est pourquoi l'absence de procédures normalisées concernant l'usage du télécopieur peut entraîner une atteinte à la confidentialité.

Il arrive que des télécopies parviennent au destinataire après les heures de travail, à un moment où les mesures de sécurité sont peut-être moins strictes et où seuls des employés de certains services sont au travail. Dans ce cas, certains organismes désignent un télécopieur particulier auquel doivent être acheminés les messages après la fermeture des bureaux. S'il est employé pour transmettre des renseignements personnels ou délicats, cet appareil devrait être placé dans un endroit verrouillé, hors de la portée des personnes non autorisées.

Les télécopies reçues par ordinateur doivent être protégées au même titre que les données personnelles ou délicates qui y sont sauvegardées. L'accès aux données devrait être contrôlé par mot de passe.

S'assurer que les télécopies parviennent à leur destinataire

La sécurité des télécopies repose essentiellement sur l'existence de politiques et de procédures adéquates de même que sur l'utilisation des caractéristiques de sécurité dont on dispose.

Contrairement au courrier envoyé à une mauvaise adresse, qui peut être renvoyé à l'expéditeur sans être ouvert, les renseignements télécopiés à un faux numéro peuvent être lus par plusieurs personnes et communiqués à d'autres. Pour éviter cette situation, les organismes devraient prendre les mesures nécessaires pour que les documents soient acheminés au bon numéro. Le numéro du destinataire devrait être confirmé avant la transmission.

Lorsqu'on utilise un télécopieur, le numéro composé est habituellement affiché. Il est donc possible de vérifier que l'on a bien composé le bon numéro avant de transmettre le document. Certains logiciels de télécopie permettent également à l'utilisateur de confirmer le numéro du destinataire avant la transmission.

Tous les logiciels de télécopie des organismes gouvernementaux devraient être en mesure d'imprimer des confirmations de transmission. L'expéditeur devrait lire la confirmation pour vérifier le numéro du destinataire. Si un télécopieur est utilisé, la confirmation devrait être conservée avec le document transmis. Si le document a été envoyé par ordinateur, l'expéditeur devrait imprimer une copie de la confirmation. Cette confirmation prouve que le document a été envoyé au bon numéro.

En cas d'envoi à un faux numéro

Si le document est envoyé par mégarde à un faux numéro, l'expéditeur devrait appeler immédiatement le destinataire, l'informer de cette erreur et lui demander de détruire le document.

Veiller à ce que la télécopie parvienne à son destinataire

Les documents envoyés au bon numéro de télécopieur ne seront pas nécessairement remis au bon destinataire. Voici la marche à suivre pour éviter ce problème :

- La première page devrait être un bordereau de transmission, qui identifie clairement l'expéditeur et le destinataire.
- Le télécopieur devrait être situé à un endroit où seules des personnes autorisées auront accès aux documents reçus.
- Les télécopies reçues par ordinateur devraient être automatiquement sauvegardées dans un répertoire auquel seul le destinataire a accès.
- Des politiques et des procédures devraient être adoptées afin que seul le destinataire prévu prenne connaissance de la télécopie.

Conclusion

La transmission de documents par télécopieur est devenue un important outil de communication. Cependant, à moins d'adopter des mesures de sécurité appropriées, l'envoi et la réception de renseignements délicats ou personnels par télécopieur risquent de donner lieu à des atteintes graves à la vie privée, à la confidentialité et à la sécurité. Il est donc avantageux pour tous les organismes d'élaborer des politiques et procédures visant à protéger les renseignements télécopiés. Il y a lieu également de sensibiliser le personnel à l'importance d'utiliser cette technologie dans le respect de la confidentialité. Le Bureau du commissaire espère que les organismes se serviront des présentes directives pour élaborer leurs propres politiques de confidentialité des communications par télécopieur.

Annexe A — Code des pratiques équitables en matière de renseignements[1]

Limitation en matière de collecte

Il conviendrait d'assigner des limites à la collecte des données de caractère personnel et toute donnée de ce type devrait être obtenue par des moyens licites et loyaux et, le cas échéant, après en avoir informé la personne concernée ou avec son consentement.

Qualité des données

Les données de caractère personnel devraient être pertinentes par rapport aux finalités en vue desquelles elles doivent être utilisées et, dans la mesure où ces finalités l'exigent, elles devraient être exactes, complètes et tenues à jour.

Spécification des finalités

Les finalités en vue desquelles les données de caractère personnel sont collectées devraient être déterminées au plus tard au moment de la collecte des données et lesdites données ne devraient être utilisées par la suite que pour atteindre ces finalités ou d'autres qui ne soient pas incompatibles avec les précédentes et qui seraient déterminées dès lors qu'elles seraient modifiées.

Limitation de l'utilisation

Les données de caractère personnel ne devraient pas être divulguées, ni fournies, ni utilisées à des fins autres que celles spécifiées plus haut, si ce n'est : a) avec le consentement de la personne concernée; ou b) lorsqu'une règle de droit le permet.

Garanties de sécurité

Il conviendrait de protéger les données de caractère personnel, grâce à des garanties de sécurité raisonnables, contre des risques tels que la perte des données ou leur accès, destruction, utilisation, modification ou divulgation non autorisés.

---

[1] Lignes Directrices Régissant la Protection de la Vie Privée et les Flux Transfrontières de Données de Caractère Personnel, <http://www1.oecd.org/dsti/sti/it/secur/prod/priv-fr.html>.

Transparence

Il conviendrait d'assurer, d'une façon générale, la transparence des progrès, pratiques et politiques ayant trait aux données de caractère personnel. Il devrait être possible de se procurer aisément les moyens de déterminer l'existence et la nature des données de caractère personnel, et les finalités principales de leur utilisation, de même que l'identité du maître du fichier et le siège habituel de ses activités.

Participation individuelle

Toute personne physique devrait avoir le droit :

a) d'obtenir du maître d'un fichier, ou par d'autres voies, confirmation du fait que le maître du fichier détient ou non des données la concernant;

b) de se faire communiquer les données la concernant :

   i) dans un délai raisonnable;

   ii) moyennant, le cas échéant, une redevance modérée;

   iii) selon des modalités raisonnables;

   iv) sous une forme qui lui soit aisément intelligible;

c) d'être informée des raisons pour lesquelles une demande qu'elle aurait présentée conformément aux alinéas a) et b) est rejetée et de pouvoir contester un tel rejet;

d) de contester les données la concernant et, si la contestation est fondée, de les faire effacer, rectifier, compléter ou corriger.

Responsabilité

Tout maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus.